Performance **T**echnology

P.O. Box 51663, Knoxville, Tennessee 37950-1663 Phone: (865) 588-1444, Fax (865) 584-3043
performtech@compuserve.com

May 2, 2002

Chairman Richard Meserve
Commissioner Nils Diaz
Commissioner Greta Dicus
Commissioner Edward McGaffigan, Jr.
Commissioner Jeffrey Merrifield
U. S. Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20872-2738

Dear Commissioners:

In my letter to the NRC Commissioners dated 10/7/99, I raised a number of safety concerns with respect to the existing NRC regulations covering commercial nuclear electric power units. One of these concerns had to do with the present regulations concerning combustible gas control. Rulemaking is presently underway for combustible gas control and this issue is close to final resolution.

Another safety concern that I raised in my letter of 10/7/99 had to do with the problem of certain equipment in a nuclear electric power unit having to react in a very short time frame. I believe certain short-term equipment response times are inappropriate and detrimental to safety. The example cited in my letter of 10/7/99 was the ten-second emergency diesel generator start time. I also believe training operators for non-realistic accidents is detrimental to safety. As indicated in the attached paper, "Are we forgetting the lessons from the accident at Three Mile Island Unit 2, March 1979 – a case study," presented April 15, 2002, at the tenth ASME International Conference on Nuclear Engineering (ICONE 10), these safety concerns still arise at the nuclear units. As the title of the paper suggests, we are forgetting the lessons learned in 1979.

Attached is a petition for rulemaking that will start to remedy the concerns with respect to very short time accidents. If implemented, this petition will delete the requirement in certain criterion in 10CFR50, Appendix A, that offsite electrical power is assumed disconnected from the nuclear unit switchyard during postulated accidents. The requirement that offsite electrical power is assumed disconnected from the nuclear unit switchyard during anticipated operational occurrences will remain.

If implemented, the proposed petition should allow the emergency diesel generator start time to be increased to a more realistic value that is not detrimental to the diesel

generator. The proposed petition should enhance operator training by eliminating some non-realistic operator training that is detrimental to safety. In my opinion, the approval of this petition for rulemaking will result in a net increase in safety at commercial nuclear electric power units in the United States.

This petition for rulemaking is submitted as part of the NRC normal practices and not part of Option 3 of SECY 98-300.

At the convenience of the Commissioners, I would be available for either discussion with individual Commissioners in your offices or at a public meeting. I will contact you in the near future to determine if you believe such discussions would be beneficial.

Sincerely,

Bob Christie

Cc: George Apostolakis, ACRS (with attachment)
Sam Collins, NRR (with attachment)
Ashok Thadani, RES (with attachment)

Performance Technology

P.O. Box 51663, Knoxville, Tennessee 37950-1663 Phone: (423) 588-1444, Fax (423) 584-3043
performtech@compuserve.com

October 7, 1999

Chairman Greta Dicus
Commissioner Nils Diaz.
Commissioner Edward McGaffigan, Jr.
Commissioner Jeffrey Merrifield
U. S. Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852-2738

Dear Commissioners:

A detailed review of the Safety Evaluation Report by the NRC staff for the San Onofre Task Zero (Pilot Program for Risk-Informed, Performance-Based Regulation) submittal of September 3, 1998 concerning the hydrogen control system convinced me that some immediate action by the NRC Commissioners would be beneficial. To this end, I request some time to talk to you about the two items listed below:

1. The San Onofre Task Zero submittal and the NRC Safety Evaluation Report. See Attachment 1 for relevant excerpts from the NRC Safety Evaluation Report and a possible NRC Commissioners' "interim" policy statement on design basis accident requirements versus severe accident information. .

2. Proposed changes to 10CFR50.44 and 10CFR50 Appendix A, General Design Criteria 41. See Attachment 2.

My purpose in requesting time to discuss these items is to start NRC Commissioner action to remedy any possible adverse conditions at the nuclear units because it is clear (at least to me) that the present regulations with regard to hydrogen control systems are detrimental to public health risk at some nuclear units and similar detrimental situations may apply to other systems as well (10 second diesel start time for example). I would be available for either discussions with individual Commissioners in your offices or at a public meeting at the convenience of the Commissioners. I will contact you in the near future to determine if you believe such discussion would be beneficial.

Sincerely,

Bob Christie

Bob Christie

Attachment to letter to NRC Commissioners from Bob Christie, dated May 2, 2002 (three page petition for rulemaking plus paper 22622 from ICONE 10)

Petition for Rulemaking

Statement of Consideration

One of the assumptions of the design basis accident analyses that is detrimental to safety is the requirement to assume a postulated accident coincident with the loss of off-site power. This requirement was placed in the regulations to try to "envelope" the worst accident such that one need not worry about lesser accidents. Details why this assumption is detrimental to safety are described in the various reports of investigatory bodies for the accident at Three Mile Island Unit 2 in 1979 (Kemeny Commission and Regovin Report) and in a paper for ICONE 10 at the end of this attachment.

The proposed changes defined below will eliminate the requirement for coincident postulated accidents and the loss of offsite-power. It will do this by changing 10CFR50, Appendix A, General Design Criteria, Criterion 17 – Electric power systems. Proposed changes to Criterion 35, Criterion 38, Criterion 41, and Criterion 44 to conform to the proposed changes to Criterion 17 are also described.

Proposed Criterion 17 - Electric power systems

An offsite electric power system and an onsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety.

The safety function for the offsite electric power system shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the reactor core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these offsite circuits shall be designed to be available in sufficient time following a loss of the other offsite electric power circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded.

The safety function for the onsite electric power system (assuming the offsite electric power system is not functioning) shall be to provide sufficient capacity and capability to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded and the reactor core is cooled and containment integrity and other vital functions are maintained in the event of anticipated operational occurrences.

The onsite electric power supplies, including the onsite batteries, the onsite electric ac power source, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their safety functions assuming a single failure.

Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies.

Proposed Criterion 35 - Emergency core cooling

A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that fuel and clad damage that could interfere with continued effective reactor core cooling is prevented.

Suitable redundancy in components and feature, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that the system safety function can be accomplished assuming a single failure. The offsite and onsite electrical power systems available to assure this system safety function shall be as described in Criterion 17.

Proposed Criterion 38 - Containment heat removal

A system to remove heat from the reactor containment shall be provided. The system safety function shall be to reduce rapidly, consistent with the functioning of other associated systems, the containment pressure and temperature following any loss-of-coolant accident and maintain them at acceptably low levels.

Suitable redundancy in components and feature, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that the system safety function can be accomplished assuming a single failure. The offsite and onsite electrical power systems available to assure this system safety function shall be as described in Criterion 17.

Proposed Criterion 41 - Containment atmosphere cleanup

As necessary, systems to control fission products, hydrogen, oxygen, and other substances which may be released into the reactor containment shall be provided, consistent with the functioning of other associated systems, to assure that reactor containment integrity is maintained for accidents where there is a high probability that fission products may be present in the reactor containment.

Suitable redundancy in components and feature, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that the system safety function can be accomplished assuming a single failure. The offsite and onsite electrical power systems available to assure this system safety function shall be as described in Criterion 17.

Proposed Criterion 44 - Cooling water

A system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink shall be provided. The system safety function shall be to transfer the combined heat load of these structures, systems and components under normal operating and accident conditions.

Suitable redundancy in components and feature, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that the system safety function can be accomplished assuming a single failure. The offsite and onsite electrical power systems available to assure this system safety function shall be as described in Criterion 17.

ICONE 10
Tenth International Conference on Nuclear Engineering
April 14-18, 2002 Arlington, Virginia

22622

"ARE WE FORGETTING THE LESSONS FROM THE ACCIDENT AT THREE MILE ISLAND UNIT 2, MARCH 1979 - A CASE STUDY."

Bob Christie
Performance Technology
P.O. Box 51663
Knoxville, TN 37950-1663 USA
Phone: (865) 588-1444 Fax (865) 584-3043
E-mail: performtech@compuserve.com

David H. Johnson
ABSG Consulting, Inc.
300 Commerce Drive, Suite 200
Irvine, CA 92602-1300 USA
Phone: (714) 734-4242 Fax (714) 734-4282
E-mail: djohnson@absconsulting.com

ABSTRACT

The accident at Three Mile Island Unit 2 in March 1979 resulted in major changes to the way emergency procedures were written and operators were trained at nuclear commercial electric generating units. These changes had a major impact on the public health risk of nuclear electric generating units. The record over the last 20 years has been excellent. For approximately 2000 reactor years of operation since 1979, there have been no accidents equivalent to TMI Unit 2 in the USA. Other factors have had an influence on this excellent record but it is clear that more efficient emergency procedures and better operator training had a significant impact on the excellent record achieved over the last 20 plus years.

Abnormal events still occur at the nuclear commercial electric generating units in the USA and these events have the potential for causing damage to the reactor core. In some cases, the emergency procedures used in abnormal events and the training received by the operators of the nuclear units have not been based on the lessons learned from the accident at Three Mile Island. The following paper describes one such case. It is clear to the authors of this paper that further changes should be made to make sure that the lessons learned from the accident at Three Mile Island Unit 2 in 1979 are implemented and not forgotten.

KEY WORDS

Operational experience, lessons learned, risk assessment, reliability requirements

INTRODUCTION

Following the accident at Three Mile Island Unit 2 in March 1979, President Carter appointed a commission to investigate the accident and make recommendations. This commission became known as the Kemeny Commission for its Chairman, Dr. John G. Kemeny, President, Dartmouth College, Hanover, New Hampshire. This Commission issued the "Report of the President's Commission on the Accident at Three Mile Island" in October 1979 (Reference 1). In the Overview of the report, the following paragraphs appear.

> "...We find a fundamental fault even with the existing body of regulations. While scientists and engineers have worried for decades about the safety of nuclear equipment, we find that the approach to nuclear safety has a major flaw. It was natural for the regulators and industry to ask: 'What is the worst kind of equipment failure that can occur.' Some potentially serious scenarios, such as the break of a huge pipe that carries the water cooling the nuclear reactor, were studied extensively and diligently, and were used as a basis for the design of plants. A preoccupation developed with such large-break accidents as did the attitude that if they could be controlled, we need not worry about the analysis of 'less important' accidents.
>
> Large-break accidents require extremely fast reaction, which therefore must be automatically performed by the equipment. Lesser accidents may develop much more slowly and their control may be dependent on the appropriate actions of human beings. This was the tragedy

of Three Mile Island, where the equipment failures in the accident were significantly less dramatic than those that had been thoroughly analyzed, but where the results confused those who managed the accident. A potentially insignificant incident grew into the TMI accident, with severe damage to the reactor. Since such combinations of minor equipment failures are likely to occur much more often than the huge accidents, they deserve extensive and thorough study. In addition, they require operators and supervisors who have a thorough understanding of the functioning of the plant and who can respond to combinations of small equipment failures."

Based on the recommendations of the Kemeny Commission and other investigating bodies, the nuclear electric power units went from emergency operating procedures based on design basis accidents to "symptom oriented" emergency operating procedures. With the new emergency procedures, operators were to base their reactions to abnormal events on equipment and procedures that led the operators to protect critical safety functions regardless of the particular circumstances of the event. In general, emergency procedures were written and operators received training on realistic events with the appropriate time sequence of these realistic events. However, in most cases, the licensing Safety Analysis Reports of the nuclear units remained tied to the design basis accidents. In some cases, operators were required to write procedures based on design basis accidents. In some cases, operators continued to receive training on the time sequence of design basis accidents. These procedures and training based on design basis accidents have resulted in the potential for ignoring the lessons learned from Three Mile Island. The following event is a case in point.

MONTICELLO LICENSEE EVENT REPORT LER 263/01-005

Licensee Event Report (LER) 263/01-005 (Reference 2), describes the following circumstances at the Monticello Nuclear Generating Plant. The Monticello plant is a Boiling Water Reactor plant with a Mark I containment and has a rating of approximately 550 Mwe. The plant is located about 30 miles outside Minneapolis, Minnesota, USA. The plant went first went critical on December 10, 1970. Commercial operation began on June 30, 1971.

On February 19, 2001, with the reactor at 100% power, the Monticello Nuclear Generating Plant staff determined that there was a need for the plant operators to manually establish torus cooling following a Design Basis Loss of Coolant Accident (LOCA) in a time shorter than the 10 minute design assumption used in the Safety Analysis Report containment analysis. The time determined to be required for operator action to meet the containment analysis requirements was closer to 6.5 minutes rather than the 10 minutes assumed in the analysis. This was due to the need to completely reflood the reactor vessel following the Design Basis LOCA prior to transferring a Residual Heat Removal pump from the injection mode to the torus cooling mode. The need for action at about 6.5 minutes was due to an emergency diesel generator loading limitation specific to certain boiling water reactors including Monticello.

Due to the relative complexity of the torus cooling evolution under design basis accident conditions, the operations staff at Monticello raised doubts as to whether the torus cooling could be completed after the core is reflooded in this compressed operating time (6.5 minutes) by the normal operating control room complement. Consequently, the containment cooling system was declared inoperable and the Limiting Condition for Operation (LCO) for containment cooling was entered. To restore operability and continue power operation, a dedicated operator was stationed in the control room with the sole purpose of initiating torus cooling during a Design Basis Loss of Coolant Accident. An operator was stationed in the control room until February 26, 2001, when the reactor was shutdown for reasons other than the operability of the containment cooling system.

Following the shutdown on 2/26/01, a solution team of Monticello staff was assembled to study torus cooling issues and recommend corrective actions. The team found that the condition described above appears to have existed since the initial licensing of the plant. The team also determined that the plant procedures that implemented the manual action to transfer the Residual Heat Removal pump were not streamlined for emergency conditions and were not written with the explicit purpose of satisfying the 10 minute design assumption. In addition, the design of the motor coolers for the Residual Heat Removal (RHR) Service Water pump required a manual action to open local motor cooling valves outside the control room prior to starting the RHR Service Water pump. Prior to the reactor startup on April 2, 2001, changes were made to the torus cooling procedure to reduce the time to initiate torus cooling. These changes included incorporation of the results of a previous calculation that had determined that the manual action of opening the RHR Service Water pump motor cooling valves could be delayed for at least 20 minutes.

The licensee performed sensitivity studies to determine the safety significance of the event. One sensitivity study was performed by personnel from General Electric on the effect of delaying torus cooling post-LOCA using the General Electric methodology used to establish the current licensing basis for containment parameters. This study showed that delaying torus cooling from ten minutes to fifteen minutes post-LOCA has an insignificant effect on the containment parameters of interest (i.e. pressure, temperature). The licensee also performed a

Probabilistic Risk Assessment on the effect of delaying torus cooling. In the Probabilistic Risk Assessment model, placing torus cooling in service within 24 hours is considered a success, and therefore the model is not sensitive to delays in initiating torus cooling on the order of minutes post-LOCA.

The licensee took the following short term corrective actions.

1. The operating procedures were revised to assure that torus cooling could be established with 10 minutes of a Design Basis LOCA. The torus cooling procedures were validated on the plant simulator under simulated Design Basis LOCA conditions. All licensed operators were evaluated in their ability to successfully complete time critical torus cooling actions. Training is being provided for all operating crews prior to assuming the watch in the plant.

2. The Monticello Emergency Operating Procedures were revised to include a statement for operators to establish containment cooling as soon as possible once adequate core cooling has been confirmed. The Emergency Operating Procedure bases were revised to reference design basis assumptions for torus cooling times. The plant staff reviewed certain accidents and licensing basis events to identify time critical operator actions. Improvements were made as needed to reinforce and control design basis assumptions.

The licensee is contemplating the following long term corrective actions.

1. Considering changes to extend the design assumption for torus cooling initiation to at least 15 minutes.

2. The torus cooling evolution is being further evaluated for changes to simplify operator actions. These changes include elimination of the need to bypass certain non-safety related interlocks.

PROBABILISTIC RISK ASSESSMENT INSIGHTS

The authors wish to amplify on the statements in the Monticello Licensee Event Report concerning the Probabilistic Risk Assessment conducted by the licensee for the event. The event is accurately described in the LER as having low safety significance in terms of public health risk. The reasons are as follows:

1. The Design Basis LOCA assumes coincident Loss of Offsite Power. This coincidence has a very low probability of occurrence.
2. The mass and energy ejected from the Reactor Pressure Vessel to the drywell during the Design Basis LOCA is immense and assumed to be done within a very short time (seconds to minutes). This mass and energy release is very overstated in terms of large Loss of Coolant Accidents as evaluated in a PRA. The reality is that these very large mass and energy assumptions in a short time are impossible in actual events.

Because of the assumptions made, as the immense amounts of mass and energy in the Design Basis LOCA get ejected into the drywell, the mass and energy get transferred to the suppression pool via relief valves in a very short time. This heats up the suppression pool and causes the torus level to rise. If the suppression pool gets too hot, the steam suppression function of the suppression pool is negated and the containment pressure and temperature rise. Ultimately the containment will fail and the steam will escape from the containment. Sooner or later there will be no water to inject into the reactor vessel without extraordinary effort by the operators. The reactor core will then melt and the fission products will escape to the atmosphere through the failed containment. To prevent such a containment failure, the Residual Heat Removal system must be transferred from the injection mode to the torus cooling mode before the suppression pool becomes too hot.

The Residual Heat Removal system is a multi-function system. During normal operation, the RHR system is in standby and not operating. Following a Design Basis LOCA, the RHR system is automatically aligned to inject water into the reactor pressure vessel from the suppression pool. The RHR system is required to restore water level in the reactor pressure vessel above the top of active reactor fuel. For the Design Basis LOCA, large amounts of water are required and consequently the RHR system is sized to restore the large amounts of water assumed lost in a short time. It takes a short time to automatically align the RHR system to the injection mode because of the requirement to start and load the emergency diesel generators in a prescribed fashion and load the RHR system pumps and have the Low Pressure Coolant Injection valves open. The RHR system pumps run in the injection mode until the reactor pressure vessel is reflooded to above the top of active fuel. This takes time because of the assumptions of the amount of original reactor water lost via the break and the assumptions concerning the diversion of injection water out of the break.

Once the reactor pressure vessel is reflooded above the top of active fuel, the RHR system pumps can be manually shifted to the torus cooling mode. Suppression pool cooling also requires operator alignment of RHR Service Water cooling to the Residual Heat Removal heat exchangers. In Design Basis LOCA assumptions, operator actions are usually not credited in the analysis for times less than ten minutes after the Design Basis LOCA. All actions taken before ten minutes must be automatic.

This Monticello Licensee Event Report exists because of the unrealistic assumptions used in Design Basis LOCA analysis. For a realistic large break Loss of Coolant Accident, the assumption of coincident Loss of Offsite power is not necessary to protect public health risk. The amount of original reactor water ejected to the drywell in a realistic large break LOCA would be much smaller than the amount lost in the Design Basis LOCA and occur over a much longer period of time. For a realistic large break LOCA, the RHR system pumps would be automatically aligned to the injection mode and injecting into the reactor pressure vessel in a short time. The amount of RHR injection water diverted to the break would be much less in a realistic large break LOCA. Recovering reactor water level to the top of active core if the RHR system were successful would be done in a short time. In a realistic large break LOCA, the suppression pool would take hours to heat up to the point where the steam suppression function is significantly impaired.

In summary, as stated in the Licensee Event Report, the event is not significant with respect to public health risk. The corrective actions described in the Licensee Event Report are driven by the assumptions as described above. Without these assumptions, the corrective actions are not necessary.

CORRECTIVE ACTIONS

The corrective actions described in the Monticello Licensee Event Report are not in agreement with the recommendations of the Kemeny Commission. The corrective actions taken show a preoccupation with Design Basis LOCAs. The corrective actions concerning training operators for short time "worst case" events is exactly what the Kemeny Commission noted as contributing to the accident at Three Mile Island Unit 2 in 1979. Revising Emergency Operating Procedures to reference design basis assumptions for torus cooling times and identifying time critical operator actions based on design basis assumptions is the same kind of thinking that contributed to the accident at Three Mile Island Unit 2.

The long term corrective actions that should be considered for this evaluation are not making adjustments to the Design Basis LOCA evaluations but rather considering what is a realistic set of requirements for Emergency Operating Procedures and operator training based on the insights of the Probabilistic Risk Assessment conducted for Monticello.

SOLUTIONS TO EVENTS SUCH AS THE MONTICELLO LER

The recommendations for improvement in Emergency Operating Procedures and operator training contained in the reports of the investigating committees for the accident at Three Mile Island Unit 2 should not be forgotten. The nuclear electric generating units should make sure that their efforts are not devoted to achieving compliance to "worst case" accidents described in the licensing of the nuclear units at the expense of more realistic accidents.

The solution to the event at Monticello does not consist of putting a reactor operator in a control room for the sole purpose of transferring a RHR valve from the injection mode to the torus cooling mode for a Design Basis LOCA. Such a solution only indicates that the basis for the decision needs revision. If the licensing basis of a nuclear unit results in such a decision, then the licensing basis needs to be changed. The need to change the licensing basis has been evident for a long time. Section 8 of the Nuclear Regulatory Commission Special Inquiry Group for Three Mile Island (Reference 3) has some excellent statements with regards to solutions.

> "...What these examples demonstrate is that we have come far beyond the point at which the existing, stylized design basis accident review approach is sufficient. The process is not good enough to pinpoint many important design weaknesses or to address all the relevant design issues. Some important accidents are outside or are not adequately assessed with the 'design envelope;' key systems are not 'safety related;' and integration of human factors into the design review is grossly inadequate.
>
> More rigorous and quantitative methods of risk analysis have been developed and should be employed to assess the safety of design and operation. But the Commission and the staff have been slow to adopt these methods, even though they have bee used in other disciplines and technologies for some years."

The ultimate solution to the types of problems considered in this case study is the change of the licensing basis. This will not be easy but it can be accomplished. It will take the combined efforts of the people at the nuclear units and the people at the Nuclear Regulatory Commission.

REFERENCES.

1. Report of the President's Commission on the Accident at Three Mile Island (Kemeny Commission), John G. Kemeny, Chairman, October 1979.

2. Monticello Nuclear Generating Plant, Docket No. 50-263, License No. DPR-22,
   Licensee Event Report 2001-005, event date 2/19/01, report date 4/19/01.

3. Nuclear Regulatory Commission Special Inquiry Group, Three Mile Island, A Report to the Commissioners and to the Public, Michael Rogovin, Director, January 1980.